

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Patent Application of:

Osamu ASANO

Application No.:

Group Art Unit:

Filed: November 14, 2003

Examiner:

For: HUB UNIT FOR PREVENTING THE SPREAD OF VIRUSES, METHOD AND  
PROGRAM THEREFOR

**SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN  
APPLICATION IN ACCORDANCE  
WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55**

Commissioner for Patents  
PO Box 1450  
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s)  
herewith a certified copy of the following foreign application:

Japanese Patent Application No(s). 2002-335409

Filed: November 19, 2002

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing  
date(s) as evidenced by the certified papers attached hereto, in accordance with the  
requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: November 14, 2003

By: 

H. J. Staas  
Registration No. 22,010

1201 New York Ave, N.W., Suite 700  
Washington, D.C. 20005  
Telephone: (202) 434-1500  
Facsimile: (202) 434-1501

日本国特許庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2002年11月19日  
Date of Application:

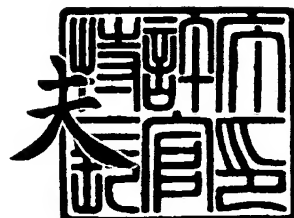
出願番号 特願2002-335409  
Application Number:  
[ST. 10/C]: [JP 2002-335409]

出願人 富士通株式会社  
Applicant(s):

2003年 7月18日

特許庁長官  
Commissioner,  
Japan Patent Office

今井 康



【書類名】 特許願

【整理番号】 0252360

【提出日】 平成14年11月19日

【あて先】 特許庁長官 太田 信一郎 殿

【国際特許分類】 G06F 9/06  
G06F 13/00  
H01L 27/00  
H04L 29/00

【発明の名称】 ウィルス拡散を防止する集線装置およびそのためのプログラム

【請求項の数】 5

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通株式会社内

【氏名】 浅野 修

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100077517

【弁理士】

【氏名又は名称】 石田 敬

【電話番号】 03-5470-1900

【選任した代理人】

【識別番号】 100092624

【弁理士】

【氏名又は名称】 鶴田 準一

## 【選任した代理人】

【識別番号】 100100871

【弁理士】

【氏名又は名称】 土屋 繁

## 【選任した代理人】

【識別番号】 100082898

【弁理士】

【氏名又は名称】 西山 雅也

## 【選任した代理人】

【識別番号】 100081330

【弁理士】

【氏名又は名称】 樋口 外治

## 【手数料の表示】

【予納台帳番号】 036135

【納付金額】 21,000円

## 【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9905449

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ウィルス拡散を防止する集線装置およびそのためのプログラム

【特許請求の範囲】

【請求項 1】 複数の通信装置を接続し該通信装置間でデータを送受信する集線装置において、

ウィルス検出情報を格納する第 1 記憶部と、

前記通信装置から受信したデータを一時蓄積する第 2 記憶部と、

前記第 1 記憶部に格納されたウィルスの検出情報に基づき、前記第 2 記憶部に一時蓄積された前記データがウィルスに感染しているか否かを判定するウィルス検出部と、

前記ウィルス検出部で前記データがウィルスに感染していると判定されたとき、該データを送信しないようにする拡散防止部と、

を備えたことを特徴とするウィルス拡散を防止する集線装置。

【請求項 2】 前記集線装置に接続された複数の通信装置の送信アドレスを格納する第 3 記憶部を備え、

前記拡散防止部は、前記ウィルス検出部で前記データがウィルスに感染していると判定されたとき、該データを送信した通信装置のアドレスを前記第 3 記憶部に格納する、

請求項 1 に記載のウィルス拡散を防止する集線装置。

【請求項 3】 前記拡散防止部は、前記ウィルス検出部がウィルスに感染していると判定したデータを検出した後、前記通信装置からの新たなデータを他の通信装置に送信しないようにする、

請求項 1 または 2 に記載のウィルス拡散を防止する集線装置。

【請求項 4】 複数の通信装置を接続し該通信装置間でデータを送受信する集線装置において、

コンピュータを、

ウィルスの検出情報を格納する第 1 記憶部、

前記通信装置から受信したデータを一時蓄積する第 2 記憶部、

前記第 1 記憶部に格納されたウィルスの検出情報に基づき、前記第 2 記憶部に

一時蓄積された前記データがウィルスに感染しているか否かを判定するウィルス検出部、および

前記ウィルス検出部で前記データがウィルスに感染していると判定されたとき、該データを送信しないようにする拡散防止部、

として機能させる、

ことを特徴としたウィルス拡散を防止する集線装置のためのプログラム。

【請求項 5】 コンピュータを、

前記集線装置に接続された複数の通信装置の送信アドレスを格納する第 3 記憶部として機能させ、かつ

前記拡散防止部が、前記ウィルス検出部で前記データがウィルスに感染していると判定されたとき、該データを送信した通信装置のアドレスを前記第 3 記憶部に格納するよう機能する、

請求項 4 に記載のプログラム。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、通信ネットワークにおけるウィルス拡散を防止する集線装置（HUB ユニット）およびそのためのプログラムに関する。

【0 0 0 2】

【従来の技術】

近年、通信技術の発展に伴いインターネット等の通信ネットワークを介したコンピュータ間および／または携帯電話間でのデータ通信が頻繁に行われるようになってきた。このようなネットワークに接続されたコンピュータに侵入し悪意に内部のデータを破壊したり外部に持ち出したりするウィルスが知られている。特に、企業内のコンピュータには機密情報が格納されているため企業にとってはウィルス対策が重要な課題になっている。このため、企業では、インターネットやイントラネットに接続された社内ホストコンピュータを外部から侵入するウィルスの感染から守るための装置（ファイアウォール）を導入している。

【0 0 0 3】

従来技術によるウイルス感染防止対策には、以下に記すようなウイルスチェックネットワークがある（下記の特許文献 1 参照）。

#### 【0 0 0 4】

このウイルスネットワークは、ネットワークに接続された個々のコンピュータにウイルス感染防止用のワクチン・ソフトウェアを導入する場合、新種のウイルスが発見される度に個々のコンピュータでその新種のウイルス対策を施したワクチン・ソフトウェアに更新しなければならず、これを各コンピュータのユーザに徹底させるのは困難であり非効率的であることから、これを効率的に行うことを目的としたものであり、ウイルスパターン格納手段と、ウイルスパターンに基づき受信したパケットがウイルス感染しているか否かをネットワーク側でチェックするウイルスチェック手段と、ウイルス感染が検出されたパケットに感染ビットを付加して該パケットを送信するパケット送信手段とを備えるウイルスチェック装置と、前記ビットに基づいて感染パケットを検出する感染パケット検出手段と、該感染パケットに対応するファイルを実行不可にするファイル実行制御手段とを備えるクライアント端末と、ウイルスパターン情報をマルチキャストで前記ウイルスチェック装置に配布するウイルスパターン情報配布手段と、前記ウイルスパターン情報を一元管理するウイルス情報管理手段とを備えるウイルス情報管理局と、を具備して構成される。

#### 【0 0 0 5】

また、他の従来技術によるウイルス感染防止対策には、コンピュータ回線網に接続されている受信側装置がコンピュータウイルスに感染した通信データを受信しないようにして受信側装置のコンピュータウイルスによる感染を未然に防ぐことを目的とし、コンピュータ回線網からデータを受信する受信処理手段と、受信データがウイルス感染しているかどうかを診断する受信データ処理手段と、受信データがコンピュータウイルスに感染している場合、これを示す感染信号を受信側装置に知らせる受信側装置間通信処理手段と、受信データがコンピュータウイルスに感染していない場合、受信データを受信側装置に送信する送信処理手段とを備えて構成したコンピュータウイルス受信監視装置およびコンピュータウイルス受信監視装置より感染信号を受信したときには受信データを受信しない受信側

装置がある（下記の特許文献2 参照）。

【0006】

【特許文献1】

特開平11-16748.7号公報（明細書の〔特許請求の範囲〕の特に〔請求項1〕と〔請求項10〕、〔発明の詳細な説明〕における段落番号〔0005〕～〔0012〕および図面の図1 参照）

【特許文献2】

特開平10-307776号公報（明細書の〔特許請求の範囲〕の特に〔請求項1〕と〔請求項3〕、〔発明の詳細な説明〕における段落番号〔0004〕～〔0014〕および図面の図1 参照）

【0007】

【発明が解決しようとする課題】

しかしながら、上記特許文献1に開示のウィルスチェックネットワークは、ウィルス感染防止のために、少なくとも伝送されるパケット（データ）にウィルス感染有無を示すビットを付すウィルスチェック装置、とそのビットに応じてウィルス侵入防止するクライアント端末と、が必須であり、全てのクライアント端末にウィルス侵入防止対策を施す必要がある。

【0008】

一方、上記特許文献2に開示のコンピュータウィルス受信監視装置もまた、コンピュータウィルス受信監視装置と受信側装置とが必須であり、全ての受信側装置に感染信号を受信したときには受信データを受信しない構成を設けなければならない。

【0009】

つまり、従来技術によれば、データを受信する全てのコンピュータに感染したデータを除去する構成を設ける必要があり、これを徹底するのは困難であるという問題を有する。

【0010】

それゆえ、本発明は、上記問題を解決し、すなわちデータを受信する全てのコンピュータにウィルス侵入防止対策を施さなくてもウィルス侵入を防止しかつウ



イルスの二次感染を防止することのできるウイルス拡散防止機能を備えた集線装置およびそのためのプログラムを提供することを目的とする。

#### 【0011】

##### 【課題を解決するための手段】

上記目的を達成する本発明のウイルス拡散防止機能を備えた集線装置は、複数の通信装置を接続し該通信装置間でデータを送受信する集線装置において、ウイルスの検出情報を格納する第1記憶部と、通信装置から受信したデータを一時蓄積する第2記憶部と、前記第1記憶部に格納されたウイルスの検出情報に基づき、前記第2記憶部に一時蓄積された前記データがウイルスに感染しているか否かを判定するウイルス検出部と、前記ウイルス検出部で前記データがウイルスに感染していると判定されたとき、該データを送信しないようにする拡散防止部と、を備えたことを特徴とする。

#### 【0012】

上記本発明のウイルス拡散防止機能を備えた集線装置において、前記集線装置に接続された複数の通信装置の送信アドレスを格納する第3記憶部を備え、前記拡散防止部は、前記ウイルス検出部で前記データがウイルスに感染していると判定されたとき、該データを送信した通信装置のアドレスを前記第3記憶部に格納する。

#### 【0013】

上記本発明のウイルス拡散防止機能を備えた集線装置において、前記拡散防止部は、前記ウイルス検出部がウイルスに感染していると判定したデータを検出した後、前記通信装置からの新たなデータを他の通信装置に送信しないようにする。

#### 【0014】

##### 【発明の実施の形態】

以下、添付図面を参照しつつ本発明の実施の形態を詳細に説明する。

#### 【0015】

図1は本発明の第一実施形態に係るウイルス拡散防止機能を備えた集線装置の概略構成図である。図1に示す集線装置1は、IEEE802.3規格で規定す

る 10BASE-T に準拠したハブ (Hub) と称するものであり、一般的にスター形の物理的トポロジーによりネットワーク装置を接続できる物理的なポートが 8 ポートや 16 ポート等、多数用意されている。ここで、ネットワーク装置とは、PC、ワークステーション、ゲートウェイ、ルータ等のコンピュータや他の集線装置を言う。

#### 【0016】

集線装置 1 は、16 ポートを有するものであり、ポート P1 に接続されたコンピュータ PC1 から受信したデータを PC1 のポート P1 を除く他の全てのポート P2 ~ P16 に (リピータハブ)、またはデータの宛先である PC が接続されているポートのみに (スイッチングハブ) 送信するための中継機能を有する。しかしながら、これらのポート P1 ~ P16 は必ずしも全て使用されない場合が多い。図 1 は 16 ポートを有する集線装置 1 に、4 ポートしかネットワーク装置 (例えば、PC1 ~ PC4) が接続されていない例を示している。また、ポート 3 とポート 4 に接続されているネットワーク装置 (例えば PC3、PC4) の電源が切れている等、集線装置 1 にケーブルが接続されていても、集線装置 1 に接続されたネットワーク装置がアクティブでない場合がある。このような場合でも、前者の集線装置 1 は、例えばポート P1 から受信したデータをポート P1 以外のポート、すなわちポート P2 からポート P16 に出力する機能を有する。

#### 【0017】

集線装置 1 は、ポート P1 ~ P16 に接続された半導体装置 (LSI) 2 を有し、LSI 2 は、ポート P1 ~ P16 が接続されるポート部 21、リピータコントローラ 22 およびウィルス処理部 23 を有する。ポート部 21 およびリピータコントローラ 22 については図 2 ~ 4 を用いて後述する。

#### 【0018】

ウィルス処理部 23 は、ウィルスのパターン情報を格納する第 1 記憶部 211 と、所定のネットワーク装置 (コンピュータ) から受信したパケットを一時蓄積する第 2 記憶部 212 と、第 1 記憶部 211 に格納されたウィルスのパターンと第 2 記憶部 212 に一時蓄積されたパケットとを比較しパケットがウィルスに感染しているか否かを判定するウィルス検出部 213 と、ウィルス検出部 213 で

パケットがウイルスに感染していると判定されたとき、パケットを集線装置 1 に接続された前記所定のネットワーク装置（コンピュータ）以外のネットワーク装置（コンピュータ）に送信しないようにする拡散防止部 214 と、各ポートに接続されたネットワーク装置（コンピュータ）の送信アドレス（MAC アドレス）を格納する第 3 記憶部 215 とを有する。ここで、MAC アドレスとは、イーサネット（登録商標）などの LAN で利用する通信回線に必要とされるもので、物理的な回線に接続されているコンピュータにセットされた LAN ボードなどを識別するためのアドレスのことである。

#### 【0019】

拡散防止部 214 は、ウイルス検出部 213 でパケットがウイルスに感染していると判定されたとき、そのパケットに付されたパケットの送信先コンピュータのアドレスが第 3 記憶部 215 に格納されている送信アドレスに一致するか否かを判定し、その結果が一致と判定されたとき、その送信アドレスに対応するコンピュータにパケットを送信しないようにするように構成してもよい。

#### 【0020】

ウイルス処理部 23 は、一般的なディジタルコンピュータからなり、図示しない双方向性バスを介して相互に接続された CPU、RAM、ROM、入力ポートおよび出力ポート等を具備する。

#### 【0021】

図 2～4 は本発明の第 1～3 実施例の集線装置を示す図であり、図 5 はリンクパルスと送受信データを示すタイムチャートである。図 2～4 に示す第 1～3 実施例の集線装置 1 は、半導体装置（LSI）2、抵抗、送信トランス、受信トランスおよびコネクタを有する。コネクタは図 1 に示すポートに相当し、図 1 に示すように、集線装置 1 に例えば PC1～PC4 のパーソナルコンピュータを接続するためのものである。LSI 2 は、n 個、本実施例では 16 個の「ポート n」と示す第 n ポート部 21n と 1 つのリピータコントローラ 22 とウイルス処理部 23 とを有する。第 n ポート部 21n は、送信ブロック 50 と受信ブロック 60 とを有する。上記抵抗、送信トランス、受信トランスおよびコネクタは、第 n ポート部 21n 毎にそれぞれ設けられている。

## 【0022】

送信ブロック50は、リンクパルス生成回路51、送信データ生成回路52、ドライバ回路53および節電回路54を有する。リンクパルス生成回路51は、リピータコントローラ22から送信される、本実施例では10MHzの送信ブロックシステムクロック（以下、単に送信クロックと記す）から図5の上段に示すようなリンクパルスを生成する。ここで、リンクパルスとは、IEEE802.3規格で定義されたものであり、図5に示すように、10ms毎に100nsのパルスを出力するものである。

## 【0023】

送信データ生成回路52は、リピータコントローラ22から送信される、送信クロック、図5の中段および下段に示すような最小64バイトから最大1500バイトの送信データおよび送信データが有効のときHighレベルとなる送信データイネーブル信号を受け、集線装置1から外部に送信する送信データを生成する。ここで、送信データは、1ビット当たり100nsのビットレートで送信されるので、最小送信データで約0.05(ms) ( $=64 \times 8 \times 100 \text{ (ns)}$ )、最大送信データで約1.2(ms) ( $=1500 \times 8 \times 100 \text{ (ns)}$ )の送信時間を要する。ドライバ回路53は、上記送信信号を増幅して出力する。

## 【0024】

節電回路54は、ドライバ回路53の出力を停止する回路であり、送信ブロック50の消費電力を削減するために設けた回路である。受信ブロック60内のリンクパルス検出回路61により検出されたリンク情報を元に、節電回路54をなすANDゲート、AND1、AND2、AND3およびAND4は制御される。リンク検出の結果がインアクティブ（この場合Low）である場合、節電回路54のANDゲートの出力はすべてLowレベルになる。この結果、リンク検出の結果がインアクティブであるポート、すなわちネットワークがアクティブでないポートの送信ブロック50の出力電流を削減することが可能になり、消費電力が削減される。次に、受信ブロック60について説明する。

## 【0025】

受信ブロック60は、リンクパルス検出回路61、PLL62、受信データ再

生回路 6 3 および送信阻止部 6 4 (図 2)、6 5 (図 3)、6 6 (図 4)を有する。リンクパルス検出回路 6 1 は、ポートを介して受信トランスから受信されるリンク情報を元に、節電回路 5 4 をなす AND ゲート、AND 1、AND 2、AND 3 および AND 4 を制御する。リンク検出の結果がインアクティブ (この場合 Low) である場合、節電回路 5 4 の AND ゲートの出力はすべて Low レベルになる。PLL (Phase Lock Loop) 6 2 は、ポートを介して受信トランスから受信された受信データから受信クロックを生成する。

#### 【0 0 2 6】

受信データ再生回路 6 3 は、リンクパルス検出回路 6 1 から受信データを PLL 6 2 から受信クロックを受け、受信データを再生するとともに受信データが有効のとき High レベルとなる受信データイネーブル信号を生成する。送信阻止部 6 4 ~ 6 6 は、ウィルス処理部 2 3 におけるウィルス検出部 2 1 3 でパケットがウィルスに感染していると判定されたとき、集線装置 1 に接続された前記所定のネットワーク装置 (コンピュータ) 以外のネットワーク装置 (コンピュータ) に送信しないようにする拡散防止部 2 1 4 の出力ポートに接続される。この出力ポートは、ウィルス感染検出前に High レベルとなり、ウィルス感染検出後に Low レベルとなる受信データディスエーブル信号を送信阻止部 6 4 ~ 6 6 に送る。

#### 【0 0 2 7】

第 2 または第 3 実施例の拡散防止部 2 1 4 は、送信阻止部 (第 2 または第 3 実施例) 6 5 または 6 6 により、ウィルス検出部 2 1 3 がウィルスに感染していると判定したパケットを検出した後、前記所定のコンピュータから新たにパケットを受信しないようにする。あるいは受信しても、他のコンピュータへ送信しないようにする。

#### 【0 0 2 8】

第 3 実施例の拡散防止部 2 1 4 は、送信阻止部 (第 3 実施例) 6 6 により、ウィルス検出部 2 1 3 がウィルスに感染していると判定したパケットを検出した後、前記所定のコンピュータから新たに受信するパケットを無効にする。

#### 【0 0 2 9】

第1～3実施例の集線装置1は、ウィルス検出部213でパケットがウィルスに感染していると判定されたとき、ウィルス感染したパケットが検出されたことを示す表示手段（図示せず）を備える。この表示によりコンピュータのユーザはウィルス感染の発生を知ることができる。

#### 【0030】

リピータコントローラ22は、第nポート部21nの何れか1つが受信した受信データ、受信データイネーブルおよび受信クロックを受け、(n-1)個の他の第nポート部21nへ送信ブロックシステムクロック、送信データおよび送信データイネーブルを送信する。

#### 【0031】

また、第nポート部21nが送信中に受信すると、送信と受信が同時となるコリージョンという状態になる。この場合、リピータコントローラ22は、次のようなコリージョン処理を実行する。全ポートにジャム信号と称する特定データを所定期間送信する。また、このコリージョンの原因となったPC側、例えばPC1、PC2も、内蔵するネットワークインターフェースカードによりジャム信号を所定期間送信する。ジャム信号が送信された後、集線装置1側およびPC側は全て送信を中止し、次いでランダム時間待った後、コリージョンの原因となったPC1、PC2は互いに時間間隔をもって送信を再開する。

#### 【0032】

次に、受信ブロック60内の送信阻止部64～66について以下に詳述する。

#### 【0033】

図2に示す第1実施例の送信阻止部64は、ANDゲートからなり、ANDゲートの一方の入力部には受信ブロック60内のリンクパルス検出回路61から送信ブロック50内の節電回路54への制御信号が、他方の入力部にはウィルス処理部23からの受信データディスエーブル信号が入力される。受信データディスエーブル信号は、拡散防止部214の出力ポートから出力され、集線装置1内のウィルス処理部23におけるウィルス検出部213でパケットがウィルスに感染していると判定されたとき、HighレベルからLowレベルに変化し、集線装置1に接続された前記所定のネットワーク装置（コンピュータ）、すなわちウイ

ルス感染したパケットを送信したネットワーク装置（コンピュータ）以外のネットワーク装置（コンピュータ）にそのパケットを送信させない。

#### 【0034】

図3に示す第2実施例の送信阻止部65は、2つのANDゲートからなり、各ANDゲートの一方の入力部には受信ブロック60内のリンクパルス検出回路61への受信信号が、他方の入力部にはウィルス処理部23からの受信データディスエーブル信号が入力される。受信データディスエーブル信号は、拡散防止部214の出力ポートから出力され、集線装置1内のウィルス処理部23におけるウィルス検出部213でパケットがウィルスに感染していると判定されたとき、HighレベルからLowレベルに変化し、集線装置1に接続された前記所定のネットワーク装置（コンピュータ）、すなわちウィルス感染したパケットを送信したネットワーク装置（コンピュータ）から新たなパケットを受信しないようにする。

#### 【0035】

図4に示す第3実施例の送信阻止部66は、ANDゲートからなり、ANDゲートの一方の入力部には受信ブロック60内の受信データ再生回路63からリピータコントローラ22への受信データイネーブル信号が、他方の入力部にはウィルス処理部23からの受信データディスエーブル信号が入力される。受信データディスエーブル信号は、拡散防止部214の出力ポートから出力され、集線装置1内のウィルス処理部23におけるウィルス検出部213でパケットがウィルスに感染していると判定されたとき、HighレベルからLowレベルに変化し、集線装置1に接続された前記所定のネットワーク装置（コンピュータ）、すなわちウィルス感染したパケットを送信したネットワーク装置（コンピュータ）から新たに受信するパケットを無効にする。

#### 【0036】

次に、集線装置1の正常状態への復帰方法について説明する。上述したように、集線装置1は、パケットがウィルス感染していることを検出すると、二次感染防止するため、受信データディスエーブル信号をHighレベルからLowレベルにしてパケットを集線装置1の外部に送信しないようにする。このような状態

になったときは集線装置 1 の筐体に取り付けた表示器（図示せず）を表示してユーザに知らせ、ユーザは例えば集線装置 1 の筐体に取り付けたりセットボタン（図示せず）を押すことによりこれを解除して正常状態にする。集線装置 1 のウィルス処理部 23 の拡散防止部 214 にこの復帰機能は設けられている。

#### 【0037】

図 6 は本発明の第二実施形態に係るウィルス拡散防止システムのブロック構成図である。図 6 全体に示すウィルス拡散防止システム 100 は、パケット（データ）通信管理部 110 と集線装置部 120 とを備える。パケット通信管理部 110 は W A N / L A N を経由した後さらに L A N を経由して集線装置部 120 に接続される。パケット通信管理部 110 は、具体的にはゲートウェイまたはルータを備える。パケット通信管理部（ゲートウェイまたはルータ） 110 には、ウィルスのパターン情報を格納する第 1 記憶部 111 a と、所定のコンピュータから受信したパケットを一時蓄積する第 2 記憶部 111 b と、第 1 記憶部 111 a に格納されたウィルスのパターンと第 2 記憶部 111 b に一時蓄積されたパケットとを比較しパケットがウィルスに感染しているか否かを判定するウィルス検出部 111 c とを備えたウィルス監視部 111 が設けられている。

#### 【0038】

ここで、ゲートウェイおよびルータは、物理層（第 1 層）、データリンク層（第 2 層）、ネットワーク層（第 3 層）、トランスポート層（第 4 層）、セッション層（第 5 層）、プレゼンテーション層（第 6 層）およびアプリケーション層（第 7 層）の 7 階層からなる、コンピュータの異機種間通信を可能とするためのネットワークアーキテクチャとしての O S I（Open Systems Interconnection；開放型システム間相互接続）の基本参照モデルにおいて、ゲートウェイはアプリケーション層の機能を果たし、ルータはネットワーク層の機能を果たす機器である。

#### 【0039】

集線装置部 120 は図 1 ～ 4 を用いて説明したものと同様な少なくとも 1 つの集線装置 121 からなる。集線装置 121 は、集線装置 121 に接続されたコンピュータの送信アドレスを格納する第 3 記憶部 122 a と、パケット通信管理部 110 のウィルス検出部 111 c でパケットがウィルスに感染していると判定さ



れたとき、そのパケットの受信先コンピュータのアドレス情報をパケット通信管理部 110 から受け、そのパケットを集線装置 121 に接続されたそのパケットの受信先コンピュータ以外のコンピュータに送信しないようにする拡散防止部 122b とを備えたウィルス処理部 122 を備える。

#### 【0040】

拡散防止部 122b は、パケット通信管理部 110 内のウィルス検出部 111c でパケットがウィルスに感染していると判定されたとき、そのパケットの送信先コンピュータのアドレス情報をパケット通信管理部 110 から受け、そのパケットに付されたパケットの送信先コンピュータのアドレスが第 3 記憶部 122a に格納されている送信アドレスに一致するか否かを判定し、その結果が一致と判定されたとき、その送信アドレスに対応するコンピュータにパケットを送信しないようにする。

#### 【0041】

集線装置部 120 は、複数個の集線装置 121 がカスケード接続されており、拡散防止部 122b は、パケット通信管理部 110 内のウィルス検出部 111c でパケットがウィルスに感染していると判定されたとき、そのパケットの送信先コンピュータのアドレス情報をパケット通信管理部 110 2 から受け、そのパケットに付されたパケットの送信先コンピュータのアドレスが第 3 記憶部 122a に格納されている送信アドレスに一致するか否かを判定し、その結果が一致と判定されなかったとき、カスケード接続された集線装置 121 で逐次上記同様の一致判定を行い、その結果が一致と判定されたとき、送信アドレスに対応するコンピュータにパケットを送信しないようにする。

#### 【0042】

図 7 は本発明の第 1 実施例のウィルス拡散防止システムを示す図である。パケット通信管理部 110 がゲートウェイ 111 であり、集線装置部 120 が 2 つの集線装置 121-1 と 122-2 を有する例を示す。集線装置 121-1 にはネットワーク装置である集線装置 1PC1、(n-1) 個のコンピュータ 1PC2、…、1PCn が接続されており、この内 1 個がルータ 112 である。集線装置 121-1 のウィルス処理部内の第 3 記憶部には各コンピュータ 1PC2、…、

1 P C n の M A C アドレスが格納されている。集線装置 1 2 1 - 2 にはネットワーク装置である m 個のコンピュータ 2 P C 1、2 P C 2、…、2 P C k、…、2 P C m が接続されている。集線装置 1 2 1 - 2 のウィルス処理部内の第 3 記憶部には各コンピュータ 2 P C 1、2 P C 2、…、2 P C k、…、2 P C m の M A C アドレスが格納されている。ここで、k、n、m は、正の整数であり、 $k < n$ 、 $k < m$  である。例えば、コンピュータ 2 P C k がウィルス感染したパケットの送信先であれば、第 1 実施例の集線装置では、集線装置 1 2 2 - 2 内のポート P k に接続された第 k ポート部 2 1 k からの送信データがディスエーブルされ、ウィルス感染したパケットは集線装置 1 2 2 - 1 および 1 2 2 - 2 の外部に出力されない。一方第 2、3 実施例の集線装置では、対応する集線装置 1 2 2 - 2 内のポート P k に接続された第 k ポート部 2 1 k への受信データがディスエーブルされ、ウィルス感染したパケットは集線装置 1 2 2 - 1 および 1 2 2 - 2 の外部に出力されない。

#### 【0043】

図 7 に示す第 1 実施例のウィルス拡散防止システムでは、パケット通信管理部 1 1 0 がゲートウェイ 1 1 1 の例として説明したが、パケット通信管理部 1 1 0 はルータ 1 1 2 であってもよい。

#### 【0044】

(付記 1)

複数の通信装置を接続し該通信装置間でデータを送受信する集線装置において

ウィルスの検出情報を格納する第 1 記憶部と、

前記通信装置から受信したデータを一時蓄積する第 2 記憶部と、

前記第 1 記憶部に格納されたウィルス検出情報に基づき、前記第 2 記憶部に一時蓄積された前記データがウィルスに感染しているか否かを判定するウィルス検出部と、

前記ウィルス検出部で前記データがウィルスに感染していると判定されたとき、該データを送信しないようにする拡散防止部と、  
を備えたことを特徴とする。

## 【0045】

## (付記2)

前記集線装置に接続された複数の通信装置の送信アドレスを格納する第3記憶部を備え、

前記拡散防止部は、前記ウイルス検出部で前記データがウイルスに感染していると判定されたとき、該データを送信した通信装置のアドレスを前記第3記憶部に格納する、

付記1に記載のウイルス拡散を防止する集線装置。

## 【0046】

## (付記3)

前記拡散防止部は、前記ウイルス検出部がウイルスに感染していると判定したデータを検出した後、前記通信装置からの新たなデータを他の通信装置に送信しないようにする、

付記1または2に記載のウイルス拡散を防止する集線装置。

## 【0047】

## (付記4)

前記拡散防止部は、前記ウイルス検出部がウイルスに感染していると判定したデータを検出した後、前記通信装置から新たにデータを受信しないようにする、  
付記1乃至3の何れか一つに記載のウイルス拡散を防止する集線装置。

## 【0048】

## (付記5)

前記拡散防止部は、前記ウイルス検出部がウイルスに感染していると判定したデータを検出した後、前記通信装置から新たに受信するデータを無効にする、  
付記1乃至4の何れか一つに記載のウイルス拡散を防止する集線装置。

## 【0049】

## (付記6)

前記ウイルス検出部で前記データがウイルスに感染していると判定されたとき、ウイルス感染したデータが検出されたことを示す表示手段を備える、  
付記1乃至5の何れか一つに記載のウイルス拡散を防止する集線装置。

## 【0050】

## (付記7)

複数の通信装置を接続し該通信装置間でデータを送受信する集線装置と該集線装置にネットワークを介して接続され前記通信装置間でデータを送受信するデータ通信管理部とを備えたウィルス拡散防止システムにおいて、

前記データ通信管理部は、ウィルスのパターン情報を格納する第1記憶部と、前記通信装置から受信したデータを一時蓄積する第2記憶部と、前記第1記憶部に格納されたウィルスのパターン情報と前記第2記憶部に一時蓄積された前記データとを比較し該データがウィルスに感染しているか否かを判定するウィルス検出部とを備え、

前記集線装置は、該集線装置に接続された通信装置の送信アドレスを格納する第3記憶部と、前記データ通信管理部の前記ウィルス検出部で前記データがウィルスに感染していると判定されたとき、該データの受信先通信装置のアドレス情報を前記データ通信管理部から受け、該データを前記集線装置に接続された前記受信先通信装置以外の通信装置に送信しないようにする拡散防止部とを備え、たことを特徴とするウィルス拡散防止システム。

## 【0051】

## (付記8)

前記拡散防止部は、前記データ通信管理部内の前記ウィルス検出部で前記データがウィルスに感染していると判定されたとき、該データの送信先通信装置のアドレス情報を前記データ通信管理部から受け、該データに付された該データの送信先通信装置のアドレスが前記第3記憶部に格納されている送信アドレスに一致するか否かを判定し、その結果が一致と判定されたとき、該送信アドレスに対応する通信装置にデータを送信しないようにする、付記7に記載のウィルス拡散防止システム。

## 【0052】

## (付記9)

前記拡散防止部は、前記ウィルス検出部がウィルスに感染していると判定したデータを検出した後、前記通信装置から新たにパケットを受信しないようにする

付記 7 または 8 に記載のウイルス拡散防止システム。

【 0 0 5 3 】

(付記 1 0)

前記拡散防止部は、前記ウイルス検出部がウイルスに感染していると判定したデータを検出した後、前記通信装置から新たに受信するデータを無効にする、付記 7 または 8 に記載のウイルス拡散防止システム。

【 0 0 5 4 】

(付記 1 1)

前記ウイルス検出部で前記データがウイルスに感染していると判定されたとき、ウイルス感染したデータが検出されたことを示す表示手段を備えた、付記 7 乃至 1 0 の何れか一つに記載のウイルス拡散防止システム。

【 0 0 5 5 】

(付記 1 2)

前記集線装置は、複数個がカスケード接続されており、

前記拡散防止部は、前記データ通信管理部内の前記ウイルス検出部で前記データがウイルスに感染していると判定されたとき、該データの送信先通信装置のアドレス情報を前記データ通信管理部から受け、該データに付された該データの送信先通信装置のアドレスが前記第 3 記憶部に格納されている送信アドレスに一致するか否かを判定し、その結果が一致と判定されなかったとき、前記カスケード接続された前記集線装置で逐次上記同様の一致判定を行い、その結果が一致と判定されたとき、該送信アドレスに対応する通信装置にデータを送信しないようにする、

付記 7 乃至 1 1 の何れか一つに記載のウイルス拡散防止システム。

【 0 0 5 6 】

(付記 1 3)

前記データ通信管理部は、ゲートウェイまたはルータである、

付記 7 乃至 1 2 の何れか一つに記載のウイルス拡散防止システム。

【 0 0 5 7 】

## (付記 14)

複数の通信装置を接続し該通信装置間でデータを送受信する集線装置において

コンピュータを、

ウィルスの検出情報を格納する第 1 記憶部、

前記通信装置から受信したデータを一時蓄積する第 2 記憶部、

前記第 1 記憶部に格納されたウィルスの検出情報に基づき、前記第 2 記憶部に一時蓄積された前記データがウィルスに感染しているか否かを判定するウィルス検出部、および

前記ウィルス検出部で前記データがウィルスに感染していると判定されたとき、該データを送信しないようにする拡散防止部、  
として機能させる、

ことを特徴としたウィルス拡散を防止する集線装置のためのプログラム。

## 【0058】

## (付記 15)

コンピュータを、

前記集線装置に接続された複数の通信装置の送信アドレスを格納する第 3 記憶部として機能させ、かつ

前記拡散防止部が、前記ウィルス検出部で前記データがウィルスに感染していると判定されたとき、該データを送信した通信装置のアドレスを前記第 3 記憶部に格納するよう機能する、

付記 14 に記載のプログラム。

## 【0059】

## (付記 16)

複数の通信装置を接続し該通信装置間でデータを送受信する集線装置において

ウィルスの検出情報を第 1 記憶部に格納し、

前記通信装置から受信したデータを第 2 記憶部に一時蓄積し、

前記第 1 記憶部に格納されたウィルスの検出情報に基づき、前記第 2 記憶部に

一時蓄積された前記データがウィルスに感染しているか否かを判定し、

前記データがウィルスに感染していると判定されたとき、該データを前記集線装置に接続された前記所定の通信装置以外の通信装置に送信しないようにする、ことを特徴としたウィルス拡散を防止する集線装置のための方法。

#### 【0060】

(付記17)

前記集線装置に接続された複数の通信装置の送信アドレスを第3記憶部に格納し、

前記データがウィルスに感染していると判定されたとき、該データを送信した通信装置のアドレスを前記第3記憶部に格納する、付記16に記載の方法。

#### 【0061】

#### 【発明の効果】

以上説明したように本発明によれば、データを受信する全てのコンピュータにウィルス侵入防止対策を施さなくてもウィルス侵入を防止しかつウィルスの二次感染を防止することのできるウィルス拡散防止機能を備えた集線装置およびそのためのプログラムを提供することができる。

#### 【図面の簡単な説明】

#### 【図1】

本発明の第一実施形態に係るウィルス拡散防止機能を備えた集線装置の概略構成図である。

#### 【図2】

本発明の第1実施例の集線装置を示す図である。

#### 【図3】

本発明の第2実施例の集線装置を示す図である。

#### 【図4】

本発明の第3実施例の集線装置を示す図である。

#### 【図5】

リンクパルスと送受信データを示すタイムチャートである。

## 【図 6】

本発明の第二実施形態に係るウイルス拡散防止システムのブロック構成図である。

## 【図 7】

本発明の第 1 実施例のウイルス拡散防止システムを示す図である。

## 【符号の説明】

- 1、121-1、121-2…集線装置
- 2…半導体装置 (LSI)
- 21…ポート部
- 21n…第 n ポート部
- 22…リピータコントローラ
- 23、122…ウイルス処理部
- 50…送信ブロック
- 51…リンクパルス生成回路
- 52…送信データ生成回路
- 53…ドライバ回路
- 54…節電回路
- 60…受信ブロック
- 61…リンクパルス検出回路
- 62…PLL
- 63…送信データ生成回路
- 64、65、66…送信阻止部
- 110…パケット (データ) 通信管理部
- 111…ウイルス監視部
- 111a、211…第 1 記憶部
- 111b、212…第 2 記憶部
- 120…集線装置部
- 122a、215…第 3 記憶部
- 122b、214…拡散防止部

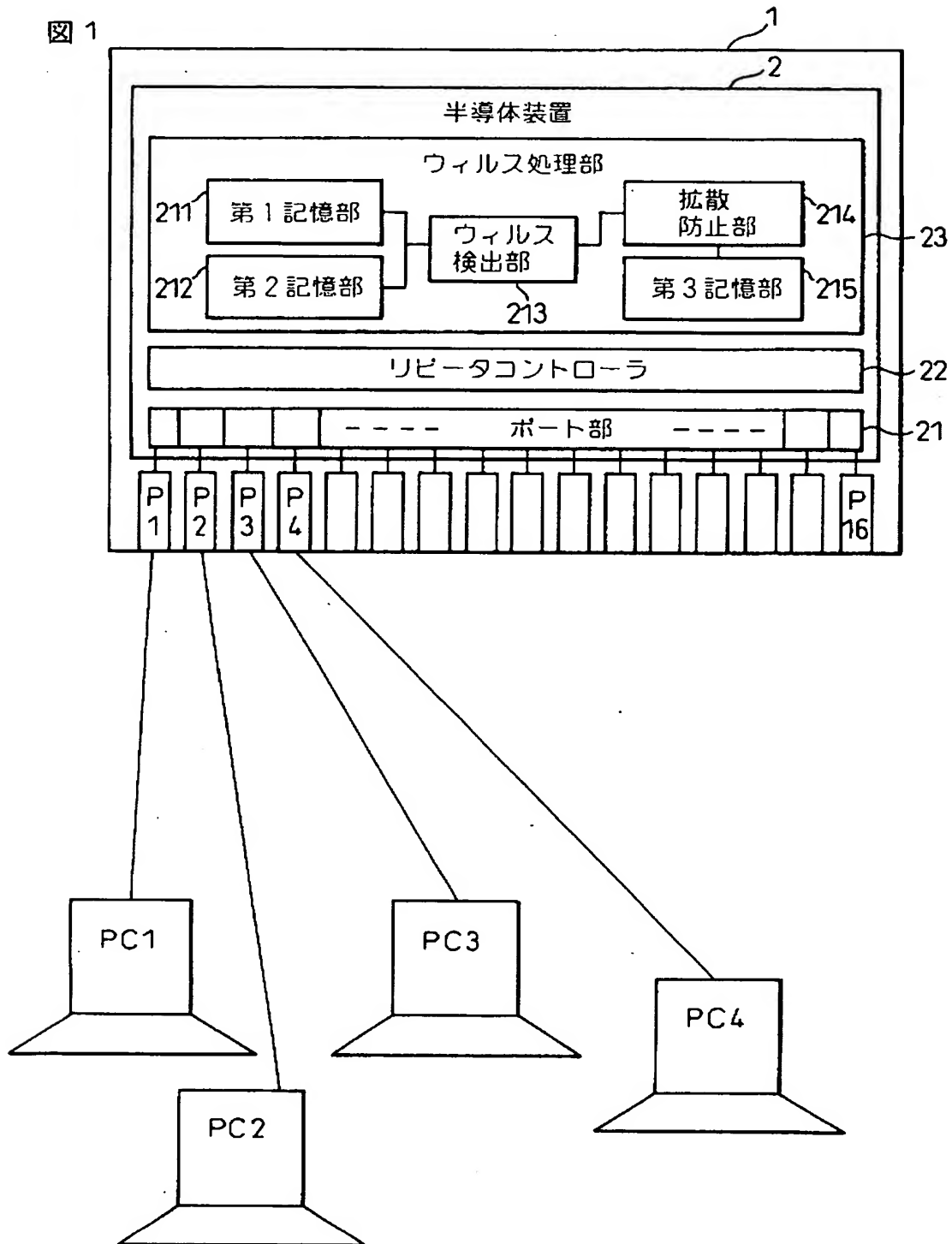


2 1 3 … ウィルス検出部

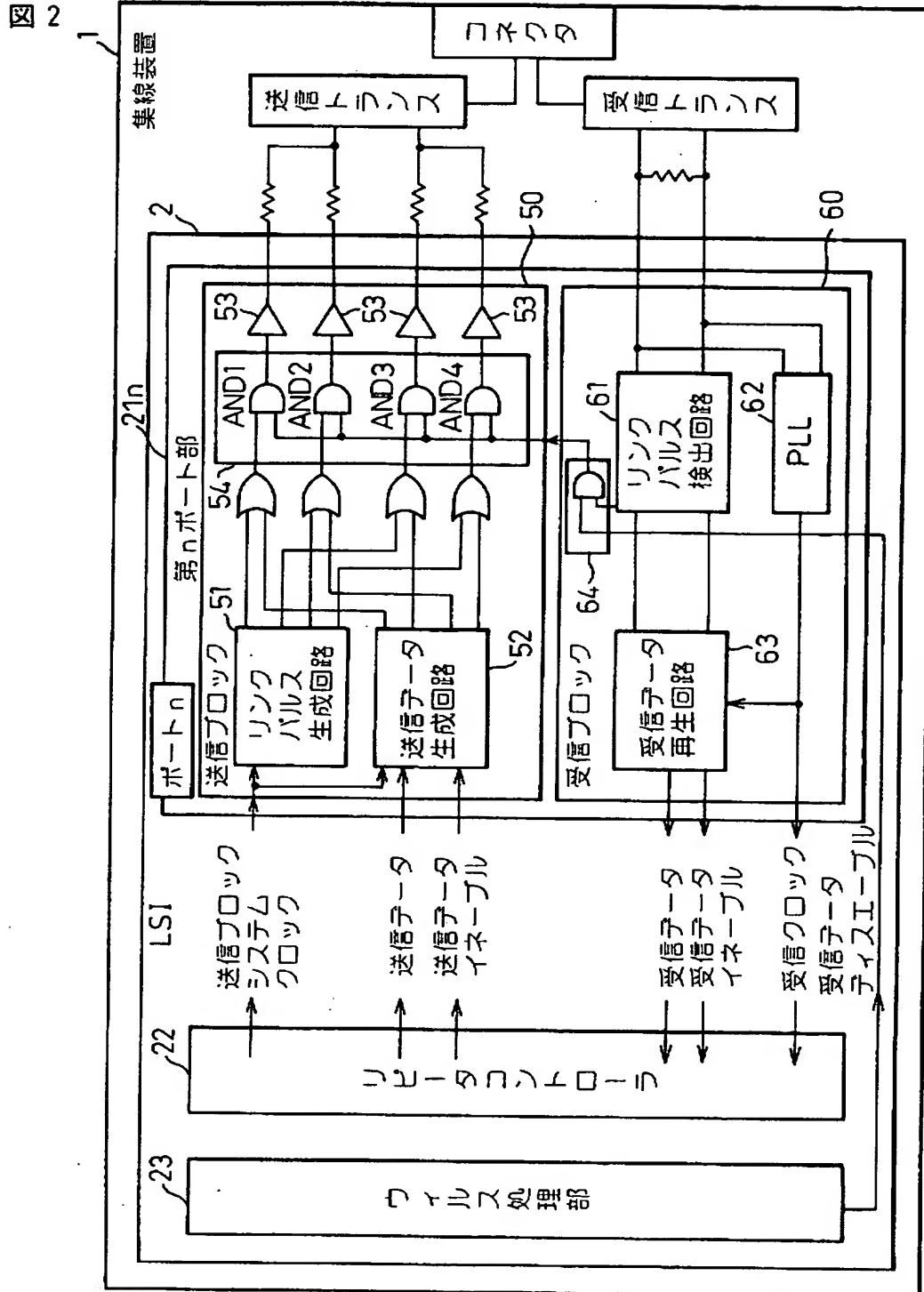
【書類名】

図面

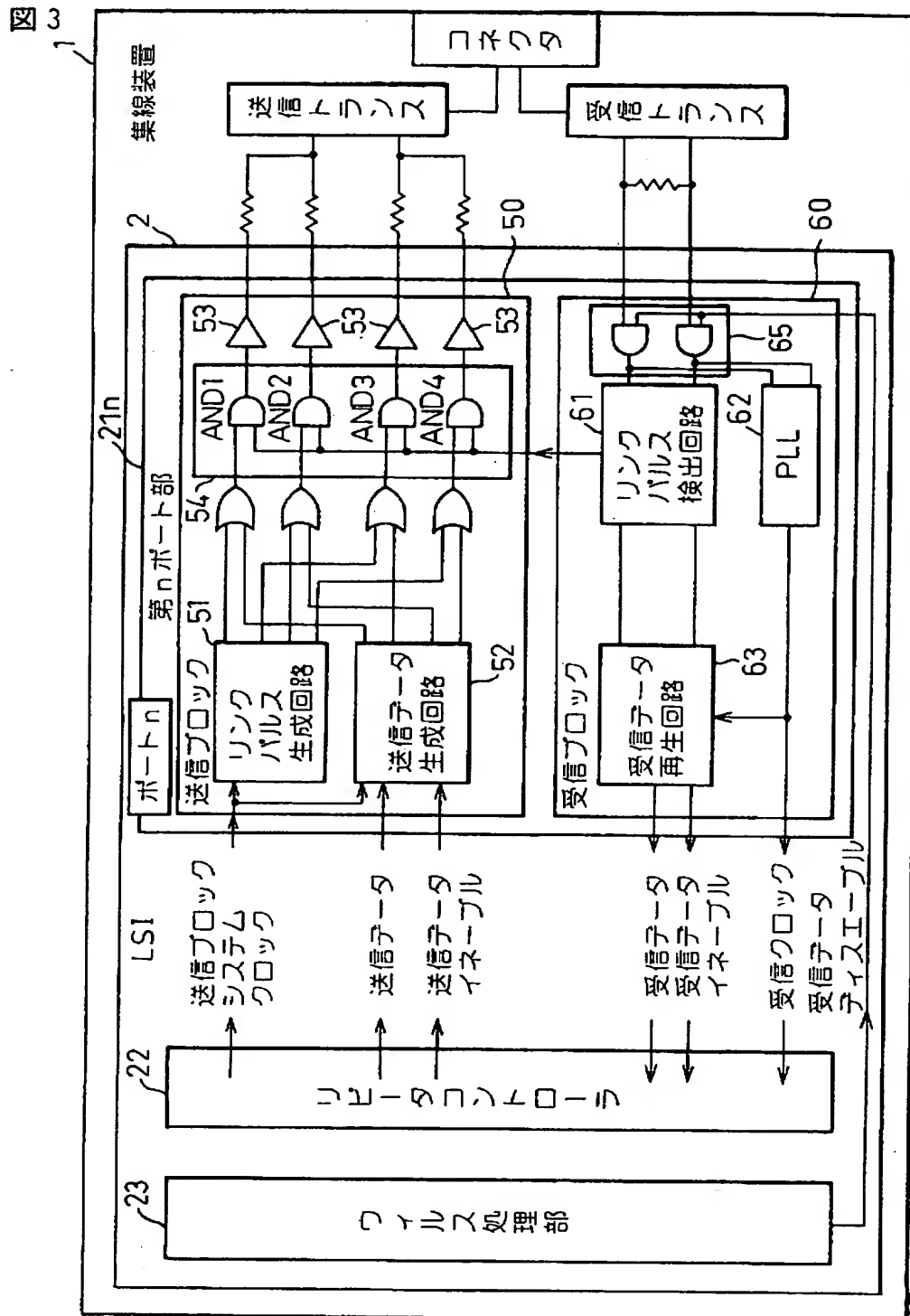
【図 1】



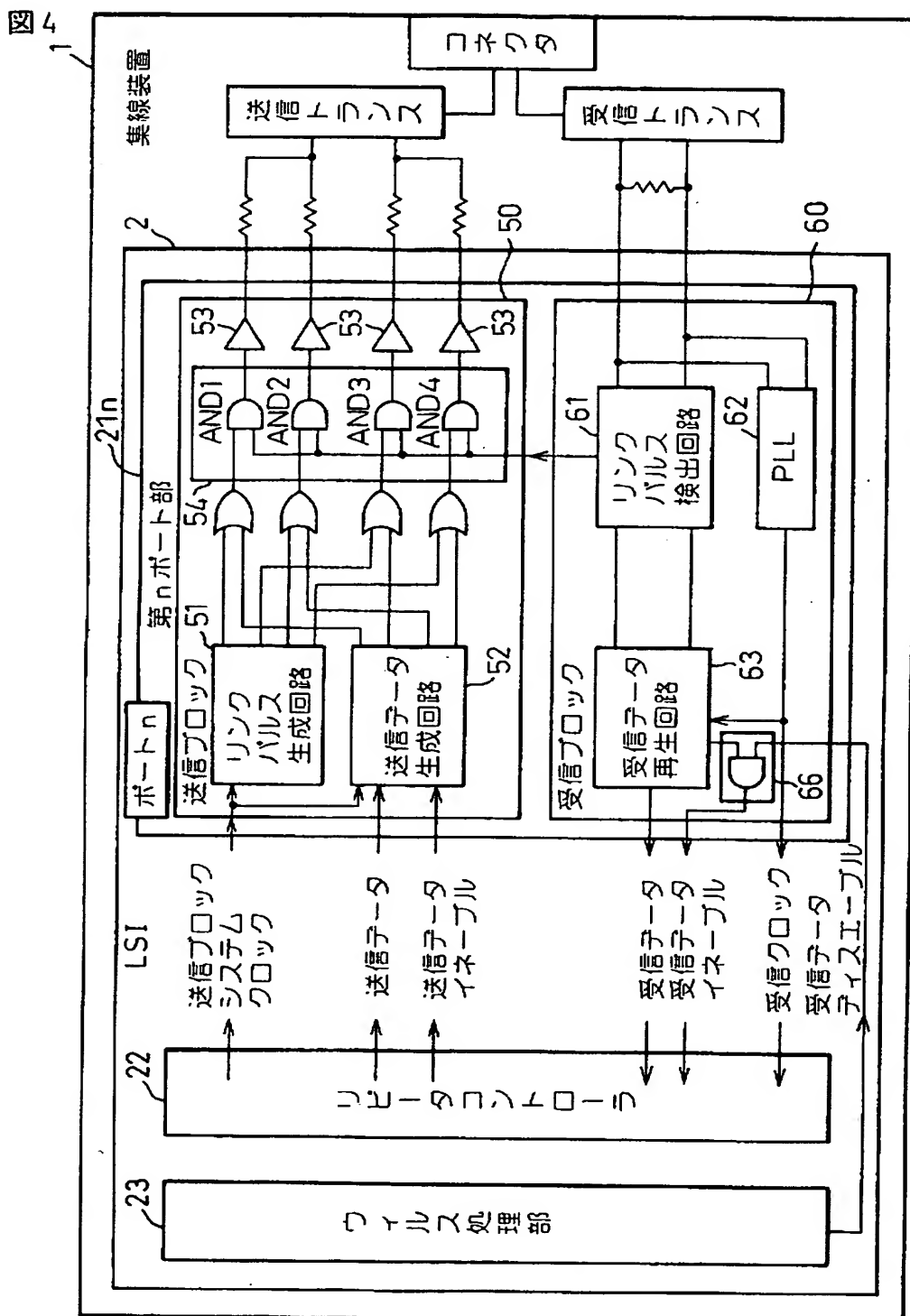
【図 2】



【図 3】

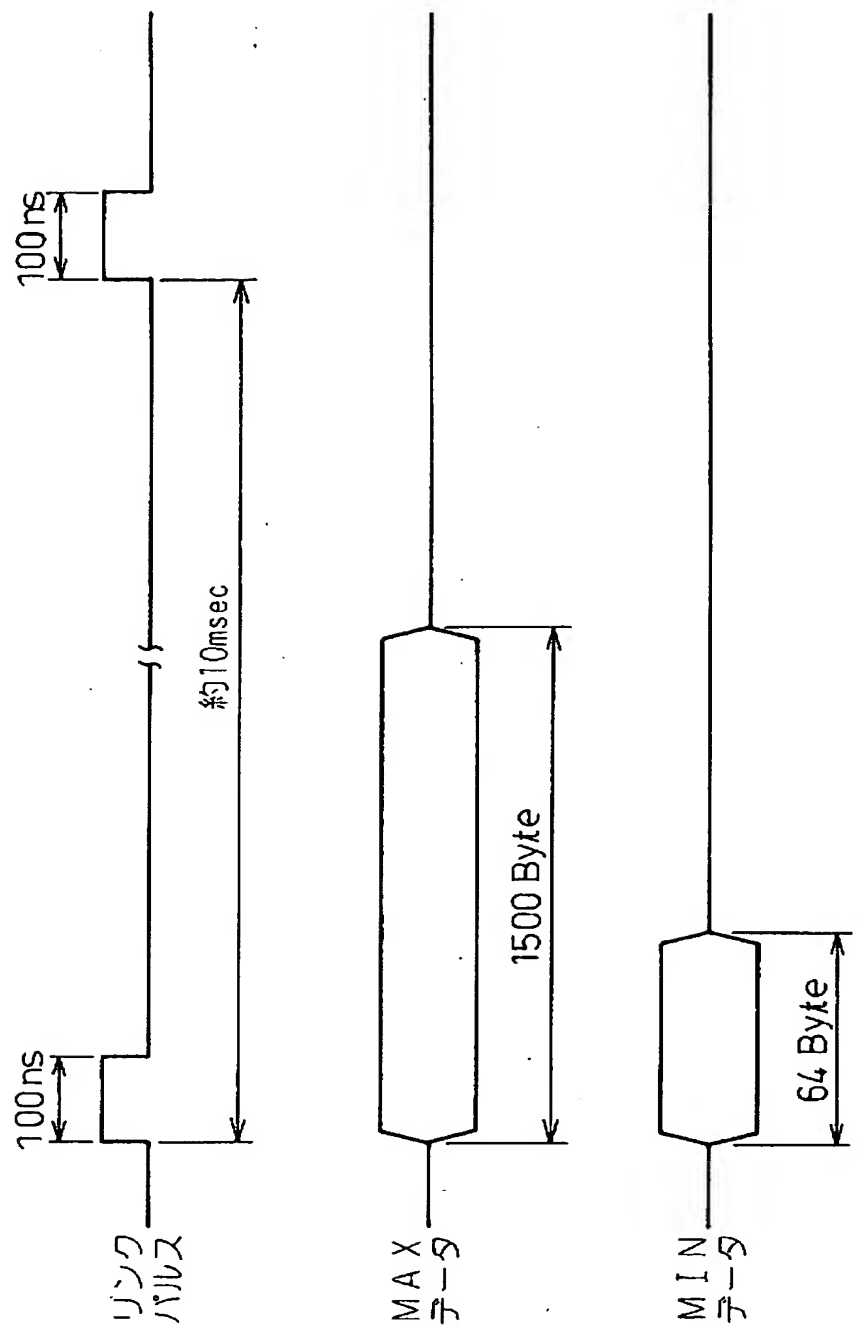


【図 4】



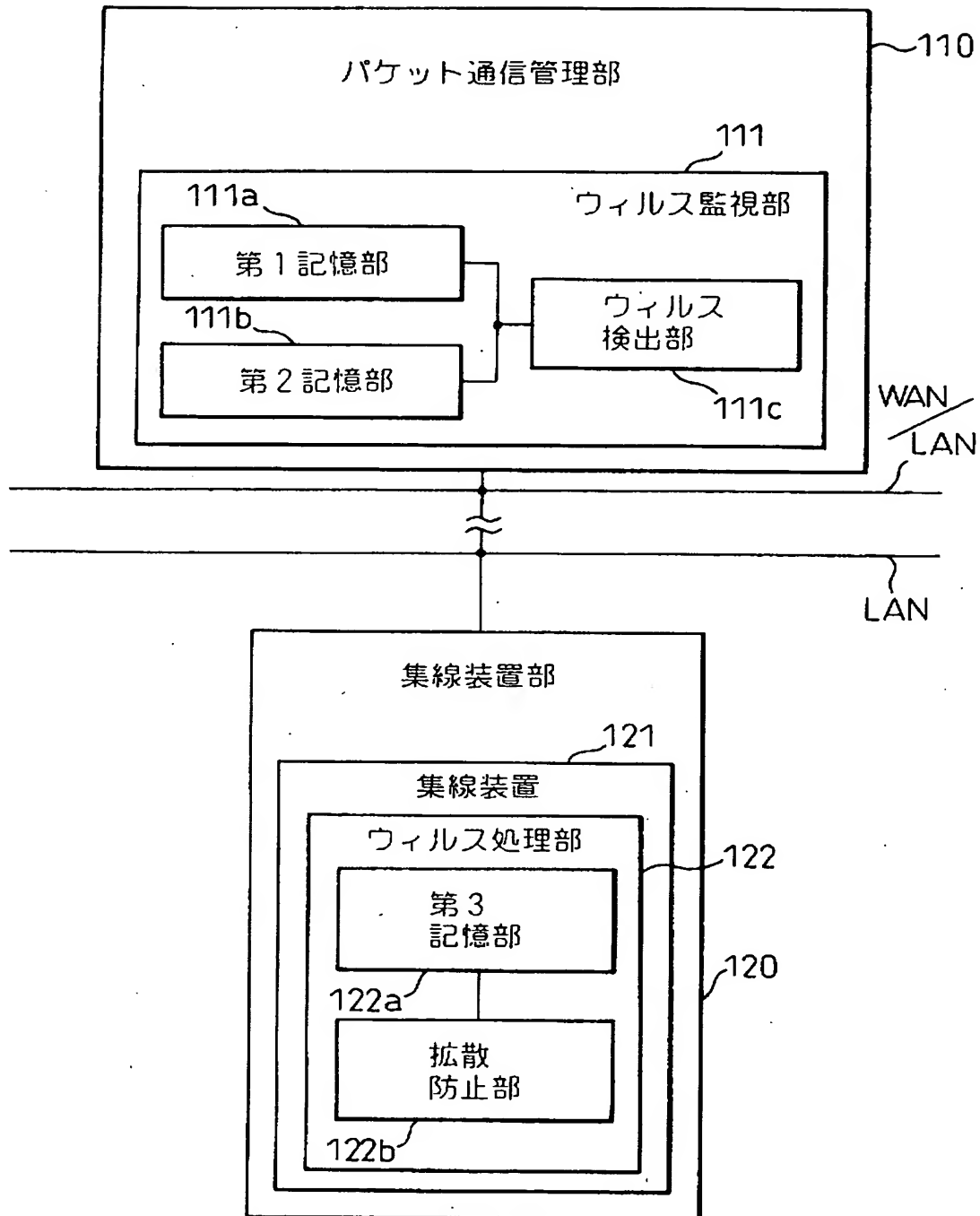
【図 5】

図 5



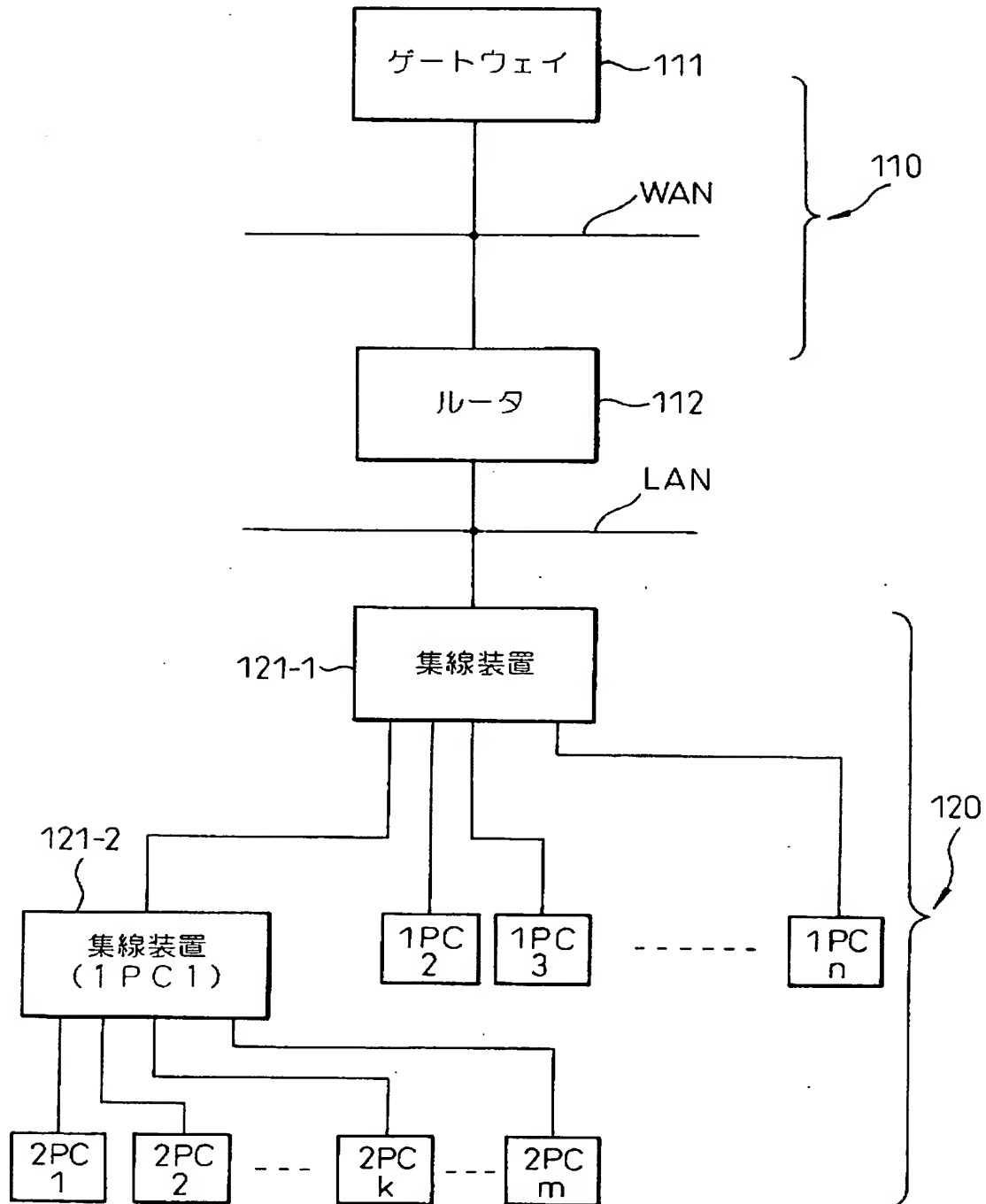
【図 6】

図 6



【図 7】

図 7





【書類名】 要約書

【要約】

【課題】 通信装置にウイルス侵入防止対策せずウイルス侵入を防止する。

【解決手段】 ウイルスの検出情報を格納する第1記憶部211、受信データを一時蓄積する第2記憶部212、記憶部211に格納されたウイルスの検出情報と記憶部212に一時蓄積されたデータとを比較しデータがウイルスに感染しているか判定するウイルス検出部213、ウイルス検出部213でデータがウイルスに感染していると判定されたとき、受信データを集線装置1の外部に送信させない拡散防止部214および集線装置1に接続された通信装置のMACアドレスを格納する第3記憶部215を備える。拡散防止部214は、データのウイルス感染と判定されたデータに付されたデータ送信先通信装置のアドレスが記憶部215に格納されているMACアドレスに一致したときそのアドレスに対応する通信装置にデータを送信させない。

【選択図】 図1

特願 2 0 0 2 - 3 3 5 4 0 9

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 5 2 2 3 ]

1. 変更年月日

1 9 9 0 年 8 月 2 4 日

[変更理由]

新規登録

住 所

神奈川県川崎市中原区上小田中 1 0 1 5 番地

氏 名

富士通株式会社

2. 変更年月日

1 9 9 6 年 3 月 2 6 日

[変更理由]

住所変更

住 所

神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号

氏 名

富士通株式会社